>_ cOSCIENZAiNrETE

Guida Galattica per newbie nel cyberspazio

Introduzione

Internet e il Web non sono la stessa cosa

Cos'è internet?

Internet è una rete di reti, il modem dentro casa tua fa parte della rete internet. È uno dei maggiori mezzi di comunicazione di massa (assieme a radio e televisione), per la sua vasta serie di contenuti potenzialmente informativi e di servizi.

Cos'è il Web?

Il **www**, (acronimo di **World Wide Web)**, spesso chiamato semplicemente **Web**, è uno dei principali servizi di internet, che permette di navigare e usufruire di un insieme molto vasto di contenuti collegati tra loro attraverso collegamenti (chiamati link) e di ulteriori servizi accessibili a tutti o ad una parte selezionata degli utenti di internet. Questa facile reperibilità di informazioni è resa possibile dai motori di ricerca e dai browser in un modello di architettura di rete definito Client-Server.

Il Web e la connessione internet sono ormai, nostro pane quotidiano. La rete è assai vasta e il suo contenuto è per la maggiorparte in inglese. **cOSCIENZAiNrETE** è una guida galattica per newbie nel cyberspazio, in italiano. È divisa in tre parti, si pone come obbiettivo principale quello di fornire una breve e pratica guida *(di sole 3 pratiche pagine e questa teorica introduzione)* per essere più coscienti quando si naviga sul Web o ci connettiamo a internet con i nostri dispositivi.

Purtroppo la maggioranza dei siti internet e servizi in rete *(es. socialnetwork, giornali, servizi metereologici e app di ogni tipo),* che usiamo tutti i giorni non sono gratuiti ma paghiamo come prezzo i nostri dati sensibili. Questi servizi non violando le norme sulla privacy per un pelo, sfruttando l'incoscienza dell'utente che cede informazioni e accetta condizioni senza sapere cosa ha effettivamente accettato.
Chi più chi meno, quasi tutti i siti stilano con degli algoritmi sempre più complessi, precisi e performanti un nostro profilo. I dati sono acquisiti in vari modi… il più semplice? Chiedendoceli attraverso semplici domande (es. "inserisci il tuo nome: "). Oppure tramite l'uso dei Cookie (hai mai letto "Questo sito utilizza cookie tecnici e di profilazione anche di "terze parti" per inviarti pubblicità e servizi in linea con le tue preferenze. Chiudendo questo banner, scorrendo questa pagina o cliccando qualunque suo elemento acconsenti all'uso dei cookie"?). Questi dati possono essere verificati, gestiti, inviati a terzi, archiviati e analizzati.

Oltre a questi servizi ci sono anche i black hat, ovvero i cosiddetti hacker cattivi. Questi rubano dati di carte di credito o dati sensibili per scopi personali o per rivenderli sui black market del DarkWeb (ben diverso dal DeepWeb); spesso per pochi spicci. In modo tale da creare identità false, utilizzando la vostra! Queste sono solo due delle tante possibili violazioni dei black hat.

Questo non accade solo sul web ma anche direttamente nei nostri PC. Utilizzando il nostro consenso o sfruttando le falle che si trovano nei sistemi operativi e software (che sugli smartphone chiamiamo app) appena si collegano alla rete internet, specie se non aggiornati all'ultima versione (contenente un livello di sicurezza maggiore). Purtroppo questo è un problema soprattutto, ma non solo, di *Microsoft Windows*. Essendo il sistema operativo più comune, è anche il più ambito dai produttori di software e black hat.

Quando in rete
sei in difficoltà,
hai dubbi
o curiosità da soddisfare,
chiedi al tuo motore di ricerca preferito
risultato garantito

estote parati

L’ESSENZIALE

1) COME SCOPRIRE SE LA/LE PROPRIE MAIL SONO STATE VIOLATE: Utilizzate il sito https://haveibeenpwned.com, scrivete la mail che volete controllare e premere su “pwned?”. Scorrere in basso per vedere su quali servizi sono state rubate le credenziali.
COME RIMEDIARE IN CASO DI PWNED: Basta cambiare password o cancellare il proprio account dai servizi in cui la propria mail è stata violata. Purtroppo per le collection (*ovvero quelle contrassegnate con il quadrato e le righe)* non esistono metodi efficaci.

2) Quando inizi ad utilizzare un nuovo servizio *(es. socialnetwork o E-Mail)* in rete e clicchi su “ho letto i termini e le condizioni d’uso”, sarebbe intelligente leggerli davvero. Potrebbe esserci scritto che rinunci alla proprietà dei tuoi dati e contenuti multimediali personali, e non solo. Pochissimo è davvero gratis, nella rete di oggi.
Hai mai notato quali autorizzazioni concedi alle tue app, non solo nel momento dell’installazione?

3) Almeno una volta ogni due settimane scansionare i dispositivi con un anti malware (come ad esempio MalwareBytes). Con le versioni a pagamento il processo è automatizzabile. [PC & Smartphone]

4) Disinstallare qualsiasi browser che non tiene alla sicurezza e privacy *(Google Chrome / Safari / Microsoft Edge / Internet Explorer / Brave / Opera)* o impararli ad usare solo per cose specifiche. Sostituendoli su smartphone con DuckDuckGo Privacy Browser,
e su PC con Mozilla Firefox che è un buon compromesso se abbinato alle estensioni (addon/componenti aggiuntivi) “DuckDuckGo Privacy Essential”, “uBlock Origin”, “HTTPS Everywhere”, “Facebook Container”, “Privacy Badger” e “Decentraleyes”.
Su alcuni smartphone Google e/o Chrome non sono disinstallabili. Basta andare su impostazioni>App>Google/Chrome>Disattiva

5) Disinstallare l’app di Facebook, poiché per usufruire del servizio social, non è essenziale. Basta aprire il browser, andare sul sito di Facebook e loggarsi. Libera spazio sullo smartphone ed è meglio in termini di sicurezza e privacy. [su smartphone]
IMPORTANTE: Quando si condivide su un qualsiasi socialnetwork un contenuto, è doveroso non fermarsi al titolo e bisogna sempre controllare se le fonti sono affidabili, in modo da non contribuire al diffondersi delle fake news.

Con InternetLiveStats
puoi conoscere quasi in tempo reale
il numero degli utenti di internet
il numero dei siti internet esistenti
quanti siti internet sono stati hackerati oggi
quanto traffico internet è stato generato oggi
e altre curiosità...

Clicca qui per visitare internetlivestats.com

LA BASE

1) Se si tiene davvero alla propria privacy in rete, bisognerebbe cancellare *(non disattivare temporaneamente),* se possibile, i propri account da tutti i Socialnetwork e dalla chat Whatsapp. Sconsigliati perché ClosedSource.
N.B.: Eliminare/disinstallare un software o una app non vuol dire cancellare il proprio account

2) È consigliato usare in alternativa la chat Telegram *(magari non con nome e cognome, come nickname)* per le svariate funzionalità e perché ha il client-side OpenSource. [PC & Smartphone]

3) Se proprio vi piacciono i socialnetwork consiglio di provare Reddit *(magari in forma anonima ovvero non con nome e cognome, come nickname).* Si trovano molte informazioni precise e quasi sempre verificate dalla community, scarseggiano le onnipresenti fake news.
Conosci A. Swartz, cofondatore di Reddit?

4) Usare un servizio E-Mail crittografato (come ad esempio ProtonMail).

E' uno strumento gratuito e opensource
in grado di testare la velocità effettiva
della tua connessione internet

Free and Open Source Speedtest. No Flash, No Java, No Websocket

Clicca qui per testare la tua velocità in rete

Clicca qui per sei link utili a saperne di più

Mastodon.uno

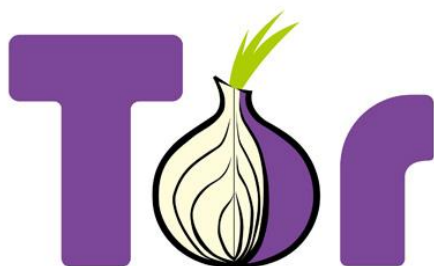
Il socialnetwork opensource decentralizzato
costituito in una federazione d'istanze

Clicca qui per dargli uno sguardo

INTRODUZIONE ALLA COSCIENZA

1) Sostituire *Microsoft Windows* (ClosedSource) con una distribuzione Linux (OpenSource). La più diffusa distro *Linux* è Ubuntu LTS, ma ce ne sono a centinaia! Un altro esempio di distro è Lubuntu che gira bene anche su PC molto vecchi.

3) Disattivare i Cookie e la cronologia per una maggiore privacy. [PC e smartphone]
Una volta disattivati, se si vuole, si possono aggiungere delle eccezioni ad i siti ai quali si vuole accedere senza ogni volta reinserire la password *[questi potrebbero essere i servizi di e-Mail (es. ProtonMail), i Socialnetwork (es. Reddit o Twitter) e le Chat (es. Telegram)]*.

4) Per avere ulteriore privacy esistono servizi a pagamento VPN *(Reti Virtuali Private)* che consentono di connettersi ad internet mascherando il proprio indirizzo IP. Una rete VPN è consigliata nel momento in cui si fa di internet uno strumento di uso aziendale/lavorativo.
Diffidare dalle VPN gratuite

Il progetto OpenSource Tor
prevede il continuo miglioramento
del browser TorBrowser

Un browser anonimo che
maschera l'indirizzo IP
tramite l'utilizzo di ponti tra reti
Serve per ricercare informazioni
sui motori di ricerca in modo
anonimo evitando il tracciamento
la sorveglianza e la censura

Clicca qui per saperne di più sul progetto Tor
IMPORTANTE: TorBrowser e Orbot (per smartphone) sono browser anonimi. Utilizzarli per accedere a qualsiasi socialnetwork o account E-Mail vanifica l'obiettivo anonimità.

Wikileaks è un'organizzazione senza
scopo di lucro destinata alla pubblicazione
e all'analisi di documenti coperti da
segreto di Stato, militare, industriale e bancario
che conserva e riceve in modo anonimo
grazie a un un potente sistema di cifratura

Wikileaks è un progetto non di proprietà Wikipedia

Clicca qui per saperne di più su Wikileaks
Scopri chi è J. Assange
Scopri chi è E. Snowden

01001001 01101100 00100000 01101100 01100001 01110100 01101111 00100000 01101111 01110011 01100011 01110101 01110010 01101111 00100000 01101000 01100001 00100000 01101001 00100000 01100011 01101111 01101111 01101011 01101001 01100101